제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

디지털 저작권 보호 기술을 이용한 라이센스 관리 기법

박복녕, 김태윤
고려대학교 컴퓨터학과
e-mail : happy@netlab.korea.ac.kr

License Administration Scheme Using Digital Copyrights Protection Technology

Bok-Nyong Park, Tai-Yun Kim
Dept of Computer Science & Engineering, Korea University

요 약

DRM에서 라이센스는 컨텐츠를 사용할 수 있는 키와 사용규칙을 포함하고 있는 사용권으로 컨텐츠의 사용과 관리를 위해서 필요하다. 이러한 라이센스에 대한 안전성을 보호하기 위해서는 안전한 키 관리 및 분배 메커니즘이 필요하다. DRM에서 컨텐츠 제작자의 저작권을 보호하기 위해서는 안전한 라이센스 획득과 라이센스 사용정보에 대한 보고가 필요하다. 본 논문에서는 DRM 시스템에서 저작권 보호 기술을 이용하여 저작권 보호를 제공하는 라이센스 관리 프로토콜을 제안한다. 제안한 프로토콜은 암호화를 통한 라이센스 획득과 라이센스 사용에 대한 지속적인 보고로 라이센스의 불법 사용 및 배포를 방지하여 디지털 컨텐츠의 제작자의 저작권을 보호한다.

1. 서론

디지털 컨텐츠 시장이 활성화되면서 디지털 컨텐츠의 불법 복제 및 배포에 대한 보호와 저작자의 저작권 보호 문제가 생겨나게 되었다. 이러한 컨텐츠 보호와 관리를 위해서는 안정성, 보안성 확보를 위한 정보보호기술과 저작권을 관리하고 컨텐츠 유통 전반을 감시 추적하는 디지털 저작권 관리(DRM, Digital Rights Management)[1][2] 기술이 필요하다.

DRM 시스템에서 사용자가 패키징된 컨텐츠를 사용하기 위해서는 제공자에게 정당한 지불을 하고 컨텐츠를 복호화 정보가 포함되어 있는 라이선스를 제공 받아야한다. 라이선스가 전달되는 과정에서 사용자 인증 및 키 분배가 발생하게 된다.

저작권의 지속적인 보호를 위해서는 컨텐츠 사용에 대한 사용정보에 대한 보고를 지속적으로 감시하고 보고 받아야 한다. 이러한 사용정보는 컨텐츠 제공자 외의 사람에게 유출되면 사용자에게 피해가 돌아갈 수도 있다. 따라서 암호화를 통해 사용자에게 컨텐츠를 제공하는 제공자에게만 안전하게 전달되어야 한다.

본 논문에서는 저작권 보호 기술을 이용한 DRM에서의 라이센스의 획득과 사용정보 보고 프로토콜을 제안한다. 참여 객체 사이의 인증과 암호화는 공개키 암호 방식을 이용한다. 제안한 프로토콜은 *ECDH(Elliptic curve Diffie-Hellman)*[3]키 설정 방식을 이용하여 세션키를 생성한다. 사용자의 장치에는 *DRM client*가 설치되어 사용자의 장치에 상주하며 라이센스의 획득과 사용에 대해 제어하고, 사용정보를 수집하여 DRM 서버에 보호하여 컨텐츠 제공자의 저작권을 보호한다.

본 논문의 구성은 다음과 같다. 2장에서는 DRM 기술 개요와 기능에 대해 소개하고, 3장에서는 논문에서 제안한 라이센스 프로토콜을 제안한다. 4장에서는 제안한 프로토콜에 대한 성능분석을 하고 5장에서는 결론을 기술한다.

2. 관련 연구

2.1 저작권 보호기술

2.1.1 암호 기술

라이센스 인증, 컨텐츠 사용자 인증, 거래 및 사용규칙 강제화, 거래 및 사용내역 확인 기능을 위하여

암호화, 전자서명, 그리고 이에 필요한 인증 및 키 분배 기술 등 다양한 암호 기술들이 사용된다. 컨텐츠는 제공되기 이전에 패키징 과정을 통해 안전한 형태로 보호된다. 컨텐츠 암호화에 사용되는 키는 안전하게 보호하기 위해서 정당한 사용자만이 접근할 수 있도록 컨텐츠 복호화 정보를 생성한다.

2.1.2 키 분배 및 관리

컨텐츠 보호를 위하여 암호화 키의 관리는 매우 중요하며, 암호화 키의 도난 방지를 위하여 엄격한 키 관리 정책 및 기술이 필요하다. DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다. 일반적으로 키 관리는 서버 기반 키 관리 방식과 분산 키 관리 방식으로 구별될 수 있다. 서버 기반 키 관리 방식은 키관리를 라이센스 발급 서버에게 집중관리 하는 방식을 말하고, 분산 키 관리 방식은 암호화키를 분산하여 관리하는 방식을 말한다.

2.2 DRM 시스템 구조

DRM 시스템은 디지털 컨텐츠 보호와 사용 규칙 관리 및 과금 체계 관리 구조로 구성된다. 그림 1은 일반적인 DRM 이용한 컨텐츠 유통 흐름도를 나타낸다[4].

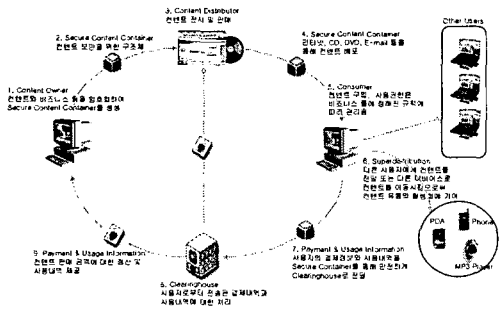

그림 1. DRM 흐름도

일반적으로 컨텐츠 보호는 디지털 컨텐츠 생성에서 배포, 사용, 폐기에 이르는 전 과정에 대해 암호화를 이용하여 가능하게 한다. 사용 규칙의 관리는 디지털 컨텐츠의 유통과 사용시 각 개인의 사용 규칙 및 권한을 정의한 것으로, 등록된 사용자는 허가된 규칙에 의해서만 컨텐츠를 사용하도록 제어할 수 있다. 마지막으로, 과금 체계 관리는 디지털 컨텐츠의 수익성을 지원하기 위해 디지털 컨텐츠의 사용 내역 관리와 이에 대한 과금 및 결재 관리 기능을 수행한다.

2.3 DRM 주요 요소 기능

DRM에서 제공하는 기능은 다음과 같다.

- 변조 방지 소프트웨어 : DRM 시스템에 대한 공격의 대부분이 사용자 모듈에서 발생한다. TRS (Tamper Resistant Software)는 DRM 클라이언트 모듈에 대한 공격으로부터 컨텐츠를 보호하는 핵심 기술로 Mocrosoft, Intertrust 등 세계의 일부 주요 DRM 업체에서 TRS 기술을 개발중이다.
- 암호 키와 안전한 컨텐츠 유통 : 암호 기술을 이용한 컨텐츠 보호와 키 분배 및 관리 메커니즘으로, 컨텐츠의 보호 및 사용 권한 정보 인증을 위한 암호화/서명 기술을 이용하여 컨테이너(Secure Container)형태로 가공한다.
- 공개키 기반 구조 : 안전한 키 관리와 사용자/클라이언트 소프트웨어 인증을 제공하여 전반적인 컨텐츠 분배 메커니즘이 안전하게 수행되도록 보장하는 기술로, DRM 기술간의 상호 운용성을 제공하기 위한 필수 조건이다.
- 디지털 워터마킹 : 컨텐츠로부터 저작권 정보(저작권자, 분배자/소비자)를 삽입하여 저작권 확인, 컨텐츠 추적 정보, 재분배자 식별(fingerprining) 기술로 향후 불법 복제 발생시 사호 구제 수단을 제공한다.
- Clearinghouse : 컨텐츠의 사용권을 부여하고 이에 대한 지속적 관리를 담당하는 시스템이 필요하게 되는데 이러한 역할을 담당하는 것이 clearinghouse이다. Clearinghouse는 전송된 결제 정보 및 사용내역을 처리해서 컨텐츠 소유자와 컨텐츠 유통업자에게 정산 금액 및 판매 내역을 제공한다.
- Superdistribution : 컨텐츠 사용자는 이 컨텐츠를 다른 사용자에게 전달 할 수 있다. 비록 구매한 이용자가 컨텐츠에 대해 사용권한을 취득한 상태라고 하더라도 전달받은 사용자가 사용규정을 만족해야만 사용권한을 부여받을 수 있다.

3. 제안한 라이센스 관리 기법

3.1 DRM Client 구조

DRM Client는 사용자 PC에 상주하여 라이선스를 발급 받고, 소유하고 있는 라이선스를 인증 받는 일을 대행하며, 컨텐츠 사용현황을 모니터링 하여 클리어링하우스에 보호하는 역할을 한다. 그림 2는 DRM Client의 구조에 대해 나타낸다.

DRM Client는 사용자 인증과 컨텐츠 접근 제어, Licence 처리, 인증에 성공했을 경우 컨텐츠 복호화, 지불, 리포팅의 모듈로 이루어져 있다. 그림 2에서와 같이 DRM Client는 제공자로부터 암호화된 컨텐츠

를 받으면 지불 후에 라이선스를 획득한다. 라이선스 획득 후 컨텐츠 이용 시 라이선스 서버에서 획득한 라이선스를 인증 받은 후 컨텐츠 복호화 키를 획득하여 컨텐츠를 이용한다. 또한 사용자의 사용현황을 기록하여 DRM 서버에 보고한다. LA는 TRS (Temper Resistance Software)[5]로 보호된다.

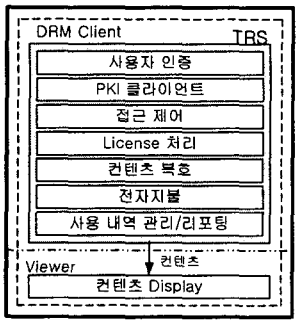

그림 2. DRM Cleint 구조

3.2 라이센스 구조

라이선스는 사용자가 컨텐츠를 이용하기 위한 컨텐츠 복호화 키와 사용규칙 등을 포함하고 있다. 논문에서 라이선스는 컨텐츠와 따로 분리되어 전달되며, 사용자가 컨텐츠를 사용하기 위해서는 반드시 지불 후에 라이선스를 전달받아야 한다.

라이선스는 라이선스 일련 번호 sn, 컨텐츠 복호화 시에 사용될 키 *Key*, 라이센스의 인증을 위한 정보인 KID=H(ID_d||License), 사용 규칙인 Usage rule, 그리고 기타 정보인 data를 가지고 있다. 이러한 파라미터들은 해수함수 H로 처리되고 라이선스 서버의 서명으로 이루어진다. KID에서 ID_d는 사용자의 특정 장치 ID로 하드웨어 바인딩을 위해 추출한다.

$$License = \{sn,\ Key,\ KID,\ Usage\ rule,\ data,\ Sig_{DRM}(H(sn,\ key,\ KID,\ Usage\ rule,\ data))\}$$

3.2 제안한 컨텐츠 저작권 보호를 위한 라이센스 관리 프로토콜

라이센스 관리 프로토콜은 라이센스를 획득 프로토콜과 라이센스 사용정보 보고 프로토콜로 이루어진다. 사용자는 라이센스 획득 단계를 통해 라이센스를 획득한 후 라이센스를 사용한다. DRM Client는 사용자의 라이센스 사용정보를 주기적으로 DRM 서버에 보고하여 라이센스의 불법 사용을 방지한다.

3.2.1 라이센스 획득 프로토콜

그림 3은 사용자 *U*에 DRM Client가 설치된 후 사용자가 다운로드한 컨텐츠에 대해 사용료를 지불한 후에 DRM 서버(*DS*)에 라이선스를 요청하여 획득하는 프로토콜이다.

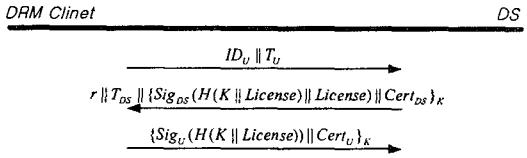

그림 4. 라이센스 획득 프로토콜

먼저 사용자는 임의의 난수 r_U를 생성하여 공개키 $T_{U=r_U}G$를 계산하고 자신의 신원 ID_U를 전송한다. ID_U는 $\{ContentID \| DID\}$로 구성된다. ID_U에서 *ContentID*는 획득할 라이센스에 관련된 컨텐츠의 *ID*이고, *DID*는 사용자의 하드웨어 장치 *ID*이다. *DID*는 하드웨어 바인딩을 위해 추출한다.

*DS*는 *U*에 설치되어 있는 *DRM Client*로부터 메시지를 받아 *U*가 등록된 사용자인지 확인하고, *ContentID*를 확인하여 이에 해당하는 라이선스를 발급한다. *DS*는 임의의 난수 r_{LS}를 생성하여 키 설정용 공개키 $T_{LS}=r_{LS}G$를 계산하여 생성한 난수 *r*과 공개키 T_U를 이용하여 *DRM Client*와 공유하는 세션키 $K=H(r_{LS}T_U \| r)$를 생성하여 자신의 개인키로 서명한 $H(K \| License)$와, 공개키로 암호화한 라이선스 *License*와 자신의 증명서를 생성한 세션키 *K*로 암호화하여 생성한 난수 *r*과 키생성용 임시 공개키 T_{LS}를 *LA*에 전송한다. *DRM Client*는 전송받은 *r*과 T_{LS}를 이용하여 세션키 $K=H(r_U T_{LS} \| r)$을 계산하여 메시지를 복호하고 서명 검증 후 라이센스를 획득한다.

라이선스를 획득한 사용자의 *DRM Client*는 사용자의 공개키 인증서와 함께 $Sig_U((H(K \| License)$을 *LS*에 보낸다.

3.2.2 사용정보 보고 프로토콜

DRM 서버인 *DS*는 *DRM Clinet*로부터 사용자의 컨텐츠 사용 현황을 보고 받는다. 이 자료는 사용자의 프라이버시가 유출될 수 있으므로 암호화하여 악

의 참여자로부터 보호되어야 한다.

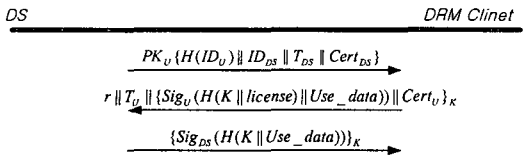

그림 5. 사용정보 보고 프로토콜

프로토콜(그림 8)이 시작되면, *DS*는 제시한 라이선스에 해당하는 컨텐츠의 사용정보를 얻기 위하여 사용자로부터 생성된 $H(ID_U)$, 자신의 식별 정보인 ID_{DS}, 세션키 설정용 임시 공개키 T_{CH}, 자신의 공개키 증명서 $Cert_{DS}$를 전송한다. 공개키 T를 계산하는 것은 3.2.1에서와 같다.

*DRM Client*는 자신의 ID_U를 해쉬처리하여 전송받은 $H(ID_U)$와 비교하여 동일할 경우 신뢰된 *DS*로부터 전송된 메시지인 것을 확인한 후 세션키 $K = H(r_U T_{CH} \| r)$을 계산하여 컨텐츠 사용정보 데이터 *Use_data*와 그 외 자료를 서명하여 세션키 K로 암호화하여 *DS*에 전송한다.

*DS*는 $K = H(r_{CH} T_U \| r)$을 계산하여 전송받은 메시지를 복호한다. *DS*는 자신이 가지고 있는 정보의 해쉬값과 $H(K \| License)$를 확인하여 통신하는 상대방이 세션키를 제대로 알고 있는지 확인하고 사용자 정보 데이터인 *Use_data*를 획득한다.

*DS*는 획득한 정보들을 $H(K \| Use_data)$로 처리하여 자신의 서명 비밀키로 서명하고 세션키 K로 암호화하여 *DRM Client*에 전송한다. 이것은 *DS*가 정상적으로 *Use_data*를 전송 받았다는 것을 확인하고, 후에 사용자의 정보가 누출되어 악용되었을 경우, 정보유출에 대한 책임에 대한 부인 방지를 위해 필요하다.

4. 성능 분석

DRM에서는 암호기술을 통해 컨텐츠 제공자의 저작권을 보호한다. 다음은 제안한 프로토콜에 대한 성능을 기술한다.

- 저작권 보호 : 제안한 프로토콜은 라이센스를 세션키로 암호화하여 전송하고 라이센스 내의 서버의 서명을 통해 라이센스의 위조 및 변조를 방지하여 라이센스를 보호하고, 라이센스의 불법 사용을 막아 디지털 컨텐츠 제작자의 저작권을 보호한다.
- 라이센스 불법 복제 방지 : 불법적인 사용자는 라이센스를 복제하여 사용할 수 있다. 그러나 라이센스 획득 프로토콜에서의 서명을 생성해낼 수 없고, 사용자의 특정 장치 키를 제시할 수 없으므로 라이센스의 복제 사용은 방지될 수 있다.
- 불법 유통 방지 : 제안한 프로토콜에서 사용하는 *DID*는 하드웨어 바인딩을 위해 추출한 사용자 장치의 고유키이다. 불법적인 사용자는 등록된 장치키와 동일 한 키를 추출하지 못하므로 $H(DID)$ 값을 생성할 수 없어 라이센스를 인증 받지 못하므로, 타 장치에서 사용을 제한하여 라이센스의 불법 유통을 방지한다.
- 사용 내역 측정 : 제안한 프로토콜에서는 *DRM Client*를 통한 사용정보 보고 프로토콜로 사용 내역을 측정하고 DRM 서버에 보고한다. 이 정보는 과금 처리를 위해 사용된다.

5. 결 론

본 논문에서는 DRM 시스템에서의 라이선스 관리를 위하여 저작권 보호 기술을 이용한 라이선스 획득과 사용정보 보고 프로토콜을 제안하였다. 제안된 프로토콜은 장치 ID를 이용해 라이선스가 특정 장치에서만 작동하도록 하여 라이선스의 불법 복제 및 사용을 방지하였고 DRM 서버를 통해 라이선스 발급 및 관리, 지불을 수행하였다. DRM 서버는 사용 내역의 주기적인 보호로 사용자의 사용 실태를 파악하여 컨텐츠의 불법 사용 감시 및 라이선스의 동적 변환이 가능하도록 하였다.

참고문헌

[1] Joshua, D., "Digital Rights Management : A Definition", IDC, 2001

[2] Joshua, D., Susan, K., "Understanding DRM System : An IDC White Paper", IDC, 2001

[3] ANSI X9.63 : Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography, ANSI, X.96-199x draft, January 1999

[4] 강호갑, "소프트웨어 저작권 보호기술", 파수닷컴 기술문서, http://www.fasoo.com

[5] Aucsmith, D., "Tamper Resistant Software: An Implementation", in Anderson, R., ed., Information Hiding, First International Workshop, Cambridge, UK., Springer-Verlag Lecture Notes in Computer Science, Vol. 1174., pp. 317-333., May 1996